ETSI ES 282 004 V3.4.1 (2010-03)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)

Reference
RES/TISPAN-02068-NGN-R3

Keywords
access, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

The present document describes the architecture of the Network Attachment Subsystem (NASS) identified in the overall TISPAN NGN architecture.

1 Scope

The present document describes the architecture of the Network Attachment Subsystem (NASS) and its role in the TISPAN NGN architecture as defined in ES 282 001 [2].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 133 203: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Access security for IP-based services (3GPP TS 33.203)".

[2] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

[3] IETF RFC 1661: "The Point-to-Point Protocol (PPP)".

[4] ISO/IEC 7498-2: "Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[5] IEEE 802.1X: "IEEE Standard for Local and metropolitan area networks - Port Based Network Access Control".

[6] ETSI TS 182 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service; Architecture and functional description [Endorsement of 3GPP TS 23.141 and OMA-AD-Presence-SIMPLE-V1-0]".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TR 121 905: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905 Release 7)".

[i.2] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

authentication: property by which the correct identity of an entity or party is established with a required assurance

NOTE: The party being authenticated could be a user, subscriber, home environment or serving network (see TR 121 905 [i.1]).

authorization: granting of permission based on authenticated identification (see ISO/IEC 7498-2 [4])

NOTE: In some contexts, authorization may be granted without requiring authentication or identification e.g. emergency call services.

Customer Network Gateway (CNG): gateway between the Customer Premises Network (CPN) and the Access Network

NOTE: A Customer Network Gateway may be in its simplest form a bridged or routed modem, and in a more advanced form be an IAD.

explicit authentication: authentication that requires that the party to be authenticated performs an authentication procedure (to verify the claimed identity of the party)

NOTE: For example, in IMS security (TS 133 203 [1]), explicit authentication is provided with full AKA directed towards the IMS client entity (represented by IMPI/IMPU and USIM/ISIM) and also implicit authentication is provided by means of the IPsec security associations.

implicit authentication: authentication based on a trusted relationship already established between two parties, or based on one or more outputs of an authentication procedure already established between two parties

line identification: process that establishes the identity of the line based on the trusted configuration

NASS user: entity requesting authorization, authentication and allocation of the IP-Address from the NASS

User Equipment (UE): one or more devices allowing a user to access services delivered by TISPAN NGN networks

NOTE: This includes devices under user control commonly referred to as CPE, IAD, ATA, RGW, TE, etc., but not network controlled entities such as access gateways.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAA Authentication Authorization and Accounting
AF Application Functions
AMF Access Management Function

AN	Access Network
API	Application Programming Interface
A-RACF	Access-Resource and Admission Control Function
ARF	Access Relay Function
ASF	Application Server Functions
ATM	Asynchronous Transfer Mode
BGF	Border Gateway Function
CLF	Connectivity session Location and repository Function
CNG	Customer Network Gateway
CNGCF	CNG Configuration Function
CPE	Customer Premises Equipment
CPN	Customer Premises Network
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EP	Enforcement Point
FQDN	Fully Qualified Domain Name
IBCF	Interconnection Border Control Function
IMS	IP Multimedia SubSystem
IP	Internet Protocol
LIF	Location Information Forum
NACF	Network Access Configuration Function
NASS	Network Attachment SubSystem
PAA	PANA Authentication Agent
PaC	PANA Client
PANA	Protocol for carrying Authentication for Network Access
P-CSCF	Proxy-Call Session Control Function
PDBF	Profile Data Base Function
PNA	Presence Network Agent
PPP	Point-to-Point Protocol
RACS	Resource Admission Control Subsystem
RCEF	Resource Control Emulation Function
TE	Terminal Equipment
UAAF	User Access Authorization Function
UE	User Equipment
VC	Virtual Circuit
VP	Virtual Path

4 General Description of NASS

4.1 High level functional overview

The Network Attachment Subsystem provides the following functionalities:

- Dynamic provision of IP address and other user equipment configuration parameters (e.g. using DHCP).
- User authentication, prior or during the IP address allocation procedure.
- Authorization of network access, based on user profile.
- Access network configuration, based on user profile.
- Location management.

The location of this subsystem in the overall TISPAN architecture can be found in ES 282 001 [2] and is shown here for information in figure 4.1.

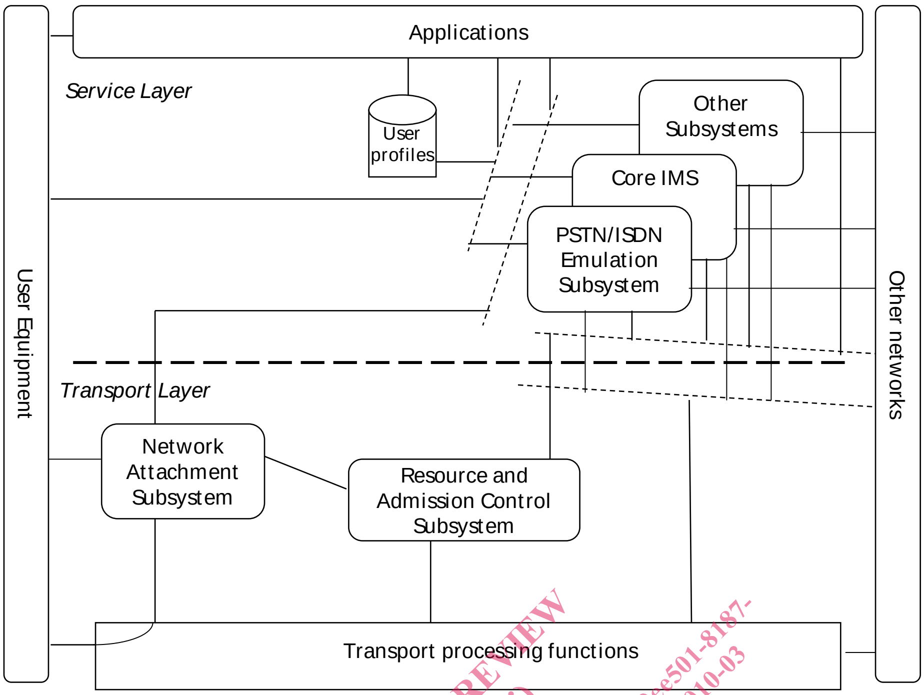

Figure 4.1: TISPAN NGN Architecture overview

4.2 High level concepts of NASS

The Network Attachment Subsystem (NASS) provides registration at access level and initialization of User Equipment (UE) for accessing to the TISPAN NGN services. The NASS provides network level identification and authentication, manages the IP address space of the Access Network and authenticates access sessions. The NASS also announces the contact point of the TISPAN NGN Service/Applications Subsystems to the UE.

Network attachment through NASS is based on implicit or explicit user identity and authentication credentials stored in the NASS.

4.3 Mobility, Nomadism

Mobility management functions provided by the NASS in the current TISPAN NGN release are limited to the ability of a terminal to be moved to different access points and access networks (which may be owned by a different access network provider) and a user to utilize different terminal, access points and access networks to retrieve their TISPAN NGN services (even from another network operator). The current TISPAN NGN release does not require the support of handover and session continuity between access networks without excluding autonomous mobility capabilities provided within the access networks.

The impact of these nomadism requirements are defined in clause 6.

4.4 Access network level registration

NASS registration involves the identification, authentication, and authorization procedures between the UE and the NASS to control the access to the NASS. Two authentication types are defined for NASS: Implicit authentication, for example based on line identification, and explicit authentication, for example based on EAP. The relationship between the identity and the credentials used for authentication must be known to the NASS for any authentication solution to be possible.

Explicit authentication is required between the UE and the NASS. It requires a signalling procedure to be performed between the UE and the NASS. Implicit authentication may be performed by the NASS based on the line identification of the connection to the UE. It is a matter of operator policy which form of authentication is applied.

Both implicit authentication and explicit authentication may be used independently as NASS authentication mechanisms.

4.4.1 Implicit authentication

Depending on the access network configuration, especially for wired broadband access networks, the implicit access authentication may rely only on an implicit authentication through physical or logic identity on the layer 2 (L2) transport layer. A UE can directly gain access to access network without an explicit authentication procedure.

A CNG shall be able to directly access an access network without an explicit authentication procedure.
Which implicit authentication method applies depends on the operator policies.

4.4.1.1 Line authentication

Line authentication is a form of implicit authentication. Line authentication ensures that an access line is authenticated and can be accessed from the CNG. Line authentication shall be based on the activation of the L2 connection between the CNG and the access network.

Line authentication ensures that an access line is authenticated and can be accessed from the CNG. The line ID shall be used for line authentication. The operator's policy shall decide whether line authentication applies.

4.4.2 Explicit authentication

In case the CNG is a routing modem and the Customer Premises Network (CPN) is a private IP realm, authentication shall be initiated from the CNG. In case the CNG is a bridge, each UE shall authenticate with the NASS as the IP realm in the CPN is known to the access network.

The relationship between the identity and the credentials used for authentication must be known to the NASS for any explicit authentication solution to be possible. The identity used for explicit authentication may depend on the authentication mechanism applied and on the access network which the UE is connected to. Two examples of these identities are:

- User identity and credentials.
- UE identity.

The type of explicit authentication mechanisms used shall depend on the access network configuration and on the operator policy.

4.4.3 CNG remote network configuration

This procedure is needed for the initialization of the CNGs accessing to the TISPAN NGN service subsystems.

4.4.4 TISPAN NGN Service/Applications Subsystems discovery

As part of the network registration process, the NASS shall have the possibility to announce the contact information of the TISPAN NGN Service/Applications Subsystems to the UE. In case the TISPAN NGN Subsystem is the IMS, the contact information provided by the NASS shall identify the P-CSCF.

The contact information provided by the NASS should either be in the form of the IP address of the contact point or in the form of the FQDN of the contact point (in which case the NASS provides the IP address of the DNS server that is able to resolve this FQDN into the IP address of the contact point).

Alternatively, the contact point to the TISPAN NGN Service/Applications Subsystems may be statically configured in the UE e.g. using Fully Qualified Domain Names (FQDN) and DNS resolution to retrieve the contact points IP addresses. This option applies in the non-roaming case.

5 Functional Architecture

5.1 Overview

The Network Attachment Subsystem (NASS) comprises the following functional entities:

- Network Access Configuration Function (NACF).
- Connectivity session Location and repository Function (CLF).
- User Authentication and Authorization Function (UAAF).
- Profile Data Base Function (PDBF).
- CNG Configuration Function (CNGCF).

The NASS has interaction with the following TISPAN NGN functional entities:

- TISPAN Service control subsystems and applications.
- Resource Admission Control Subsystem (RACS).
- Access Relay Function (ARF) and Access Management Function (AMF).
- User Equipment (UE).

One or more functional entities may be mapped onto a single physical entity. If one functional entity is implemented by two physical entities, the interface between these physical entities is outside the scope of standardization.

Functional entities in the Network Attachment Subsystem (NASS) may be distributed over two administrative domains. See clause 6 for the impact of roaming on the distribution of NASS.

Figure 5.1 provides an overview of the relationships between these functional entities and other subsystems of the NGN architecture. Interfaces to charging systems are not represented. Annex A provides informative, potential physical configurations in which the functional NASS architecture can be applied.

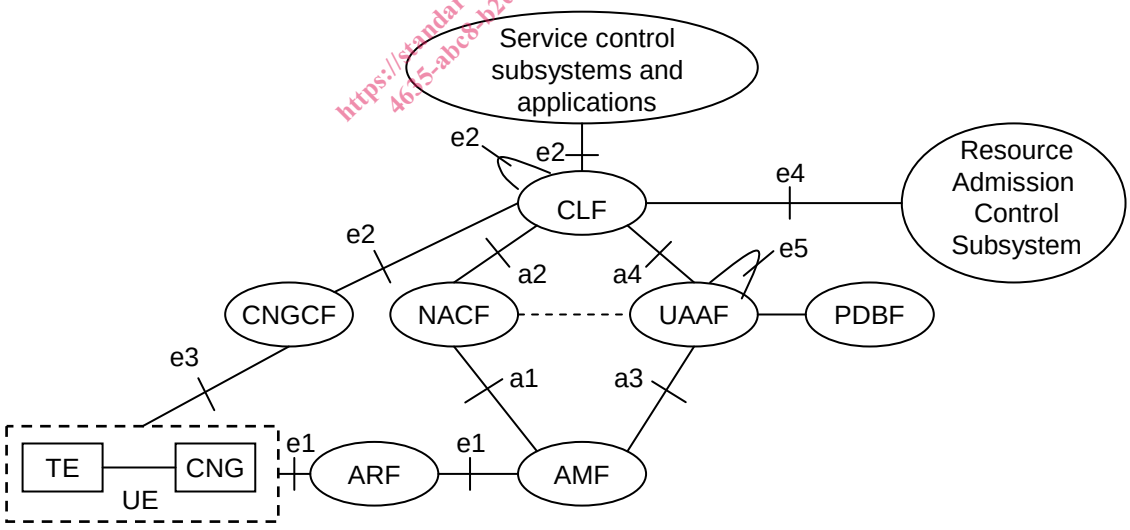

Figure 5.1: Network Attachment Subsystem architecture

5.2 Functional Entities

5.2.1 Network Access Configuration Function (NACF)

The Network Access Configuration Function (NACF) is responsible for the IP address allocation to the UE. It may also distribute other network configuration parameters such as address of DNS server(s), address of signalling proxies for specific protocols (e.g. address of the P-CSCF when accessing to the IMS).

The NACF should be able to provide to the UE an access network identifier. This information uniquely identifies the access network to which the UE is attached. The UE may send this information to applications as a hint to locate the CLF.

NOTE 1: The transport of the access identifier depends on extension in existing protocols (e.g. new DHCP option or usage of DHCP option 120). If NASS does not have the means to convey this parameter to the UE, this function will not be supported.

NOTE 2: DHCP servers or RADIUS servers are typical implementations of the NACF.

5.2.2 Void

5.2.3 Connectivity session Location and repository Function (CLF)

The Connectivity session Location and repository Function (CLF) registers the association between the IP address allocated to the UE and related network location information provided by the NACF, i.e.: access transport equipment characteristics, line identifier (Logical Access ID), IP Edge identity, etc. The CLF registers the association between network location information received from the NACF and geographical location information. The CLF may also store the identity of the NASS User to which the IP address has been allocated (information received from the UAAF), as well as the associated network QoS profile and preferences regarding the privacy of location information. In case the CLF does not store the identity/profile of the NASS User, the CLF shall be able to retrieve this information from the UAAF. For detailed CLF information model and state model see clauses 5.2.3.1 and 5.2.3.2.

The CLF responds to location queries from service control subsystems and applications. The actual information delivered by the CLF may take various forms (e.g. network location, geographical coordinates, post mail address etc.), depending on agreements with the requestor and on NASS User preferences regarding the privacy of its location. Any privacy information, that may indicate a level of accuracy of the location information to be delivered, is also sent with the actual location information.

NOTE 1: The implications and impacts of the extension of allowing the privacy indication to be sent over the e2 reference point to the application service control function on functions in the application layer and from the access (PBX networks etc.) are FFS.

NOTE 2: The decision over allowing this to change earlier versions of the present document as an essential change is FFS.

NOTE 3: The retrieval by the CLF of geographical information from related NASS User network location characteristics is outside of the scope of the present document.

NOTE 4: Geographical information may take several different forms depending on the access type and the application. The definition of this format shall also be lined up with OCG EMTEL who has decided that the LIF (Location Information Forum) is required in certain environments according to regulatory requirements. This data field is intended to be a placeholder for this information

The CLF interfaces with the NACF to get the association between the IP address allocated by the NACF to the NASS User and the Line ID.

The CLF also registers NASS User network profile information (received from the UAAF at authentication) to make this profile information available to the RACS at authentication of the UE.

The CLF is able to correlate the information received from NACF and UAAF based on the Logical Access ID.

5.2.3.1 Information Model

The CLF holds a number of records representing active sessions. These records contain information received from the NACF and the UAAF, information on the list of AFs having subscribed to particular events, and additional statically configured data. The following table identifies which information elements are stored for each of these sessions

NOTE: In case PPP is used the Physical access ID may be provided from the UAAF to the CLF.

Table 5.1

Access Session Description	
Information Received from the NACF	
Globally Unique Address	
- Assigned IP Address	The IP address of the attached NASS User.
- Address Realm	The addressing domain in which the IP address is significant.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
Logical Access ID	The identity of the logical access used by the attached NASS User. In the xDSL case, the Logical Access ID may explicitly contain the identity of the port, VP and/or VC carrying the traffic.
Terminal Type	The type of user equipment to which the IP address has been allocated.
Information Received from the UAAF/PDBF	
NASS User ID	The identity of the attached NASS User.
Logical Access ID	The identity of the logical access used by the attached NASS User.
Physical Access ID (optional)	The identity of the physical access to which the NASS User is connected.
CNGCF Address (optional) (see note 6)	The address of the CNGCF entity from which configuration data may be retrieved by the user equipment.
P-CSCF Identity (optional) (see note 7)	The identity of the P-CSCF for accessing IMS services.
Privacy Indicator	Whether location information can be exported to services and applications (see note 1).
QoS Profile Information (see notes 2 and 3)	
- Transport Service Class	The transport service class subscribed by the attached NASS User. The transport service class relates to a forwarding behaviour at the transport plane.
- Media Type	The media type(s) to which the QoS profile applies.
- UL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the uplink direction.
- DL Subscribed Bandwidth	The maximum amount of bandwidth subscribed by the attached NASS User in the downlink direction.
- Maximum priority	The maximum priority allowed for any reservation request.
- Requestor Name	Identifies the requestor(s) allowed by the QoS profile.
Initial Gate Settings (optional)	
- List of allowed destinations as well as multicast flows	In case of unicast data, the list of default destination IP addresses and/or ports and/or port-ranges and/or prefixes to which traffic can be sent. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs which traffic can be received from by the attached NASS User. Address ranges are supported within the list (see note 4).
- List of denied destinations as well as multicast flows	In case of unicast, the list of default destination IP addresses, ports, prefixes and port ranges to which traffic is denied. In case of multicast, the list of IP-Multicast group addresses and/or the list of (Source IP address, IP-Multicast group address) pairs for which traffic towards the attached NASS User must be denied. Address ranges are supported within the list (see note 4).